

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

STRATEGY RESEARCH PROJECT

CRYPTOGRAPHY, INFORMATION OPERATIONS AND THE INDUSTRIAL BASE: A POLICY DILEMMA

BY

LIEUTENANT COLONEL STEPHEN C. HORNER
United States Army

DISTRIBUTION STATEMENT A:

**Approved for public release.
Distribution is unlimited.**

19970623 259



USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

**CRYPTOGRAPHY, INFORMATION OPERATIONS AND THE INDUSTRIAL
BASE: A POLICY DILEMMA**

by

Lieutenant Colonel Stephen C. Horner

Colonel Nathan Bard
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DISTRIBUTION STATEMENT A:
Approved for public
release. Distribution is
unlimited.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Stephen C. Horner (LTC), USA

TITLE: Cryptography, Information Operations and the Industrial Base: A Policy Dilemma

FORMAT: Strategy Research Project

DATE: 7 April 1997 PAGES: 34 CLASSIFICATION: Unclassified

The information age is in full swing and it is changing the face of national security. The explosive force of information technology places the Global Information Infrastructure, the worldwide industrial base and the various world governments in both mutually supporting and somewhat adversarial positions. The information infrastructure is rapidly becoming the lifeblood for the world's industry and a critical part of the national infrastructure around the world. Consequently, the emerging operational regime of information operations is playing a critical role in the protection of U.S. national security interests and exploitation of adversary systems associated with information systems. Cryptography, long a traditional government area of interest, is taking on increased importance in industry, not only for protection of sensitive data but as a worldwide product market itself. The U.S. government cryptography policy must balance the need for continued U.S. dominance in information technology and the government's legitimate need to access data. U.S. dominance requires increased access to world markets for U.S. cryptography technology. Solution to this policy dilemma requires a team approach by U.S. government and industry to provide the best answer.

TABLE OF CONTENTS

TABLE OF CONTENTS	v
INTRODUCTION	1
THE CHANGING FACE OF NATIONAL SECURITY	2
THE INFORMATION INFRASTRUCTURE.....	2
THE INDUSTRIAL BASE AND THE INFORMATION INFRASTRUCTURE	6
INFORMATION OPERATIONS	8
CRYPTOGRAPHY'S NOT JUST FOR UNCLE SAM ANYMORE	10
THE INDUSTRY PERSPECTIVE	11
THE GOVERNMENT PERSPECTIVE.....	13
THE CRYPTOGRAPHY POLICY DILEMMA	14
FOCUS ON ACCESS	15
WORKING ON THE ISSUES.....	17
WHAT SHOULD THE U.S. DO?	20
CONCLUSION	24
ENDNOTES	25
BIBLIOGRAPHY	27

Introduction

The information age is in full swing and the United States is at the forefront. The U.S. government and industry are key players in and ardent supporters of the rapidly developing National Information Infrastructure (NII) and the Global Information Infrastructure (GII). The protection of the GII and NII and their associated data is increasingly important as they become more intertwined with the national security interests of the U.S. The specter of information warfare on these information super highways provides a policy dilemma for the U.S. government as it both recognizes the need to protect the industrial base's information security and provide for the ability to protect U.S. national security. Cryptography is a major element in this dilemma as national security considerations have been the overwhelming drivers for all policy and activities involving cryptography. The U.S. government and industry must deal with the emerging information technology revolution and its attendant implications. Industry views cryptography as a shield for its sensitive information and a product for the information technology market. The government recognizes it must protect cryptography technology and view it in light of the Information Operations regime and other national power considerations. This collection of circumstances poises a policy dilemma for the U.S. government as it must balance national security considerations with industry desires and requirements within the constantly evolving information technology environment.

We will discuss four key points in looking at this dilemma. First, we will look at the changing face of national security in the information age. How do the information infrastructure, the industrial base and information operations interact to change the way

we look at national security? Second, in light of this change comes the realization that cryptography is not just for Uncle Sam anymore. The drivers are national security and economics combined under the pressure of globalization characteristics: interconnectivity and markets. Third, that the two points above create a difficult policy dilemma for the U.S. The U.S. government and industry stake in the cryptography arena represents that dilemma. Finally, what should the U.S. do in resolving this dilemma? Is there a solution that will satisfy everyone?

The Changing Face of National Security

National security, for many years, conjured up images of armed forces, defense of the homeland, possessions, or allies, safe passage in sea, air, or space, or protection of vital interests. The information age adds a new dimension for national security and alters the way we think of national security forever. The combination of the information infrastructure, the industrial base and the new operational regime of information operations makes national security a significantly more complex and dynamic arena.

The Information Infrastructure

The National Information Infrastructure and the Global Information Infrastructure are the “information super highways” so often referred to in today’s literature. The exploding information technology field has virtually propelled the U.S. and other countries’ national and economic elements into a new environment. An environment where the immediate access to or transmission of vast amounts of data is becoming an accepted everyday occurrence not just for large corporations, organizations or

governments but for small groups and individuals also. Their embedded nature makes border identification virtually impossible on the GII, NII or even DII (Defense Information Infrastructure).¹

The draft Joint Pub 3-13, Joint Doctrine for Information Operations, dated 21 January 1997, defines the GII as “the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers and much more.”² It also states that the NII characteristics are the same as the GII but with a national level focus. According to Joint Pub 3-13, the DII focuses on DoD local, national and worldwide military matters and includes all systems, to include commercial, carrying DoD information.³

The recently released U.S. Army Field Manual (FM) 100-6, Information Operations expands this when it discusses the Global Information Environment (GIE) that enfolds the GII, NII and DII. It defines GIE as “all individuals, organizations or systems, most of which are outside the control of the military or National Command Authorities, that collect, process and disseminate information to national and international audiences.”⁴ FM 100-6 further makes the point that the GIE “is both interactive and pervasive in its presence and influence”⁵ and “as technology enables greater numbers of individuals, groups, organizations and nation-states to be linked to the

world through the GIE, these users can be expected to pursue their own interests by attempting to manipulate and control information's control and flow”⁶

Many of the elements of these definitions have been around for years and are not startling new discoveries. It is the widespread access and evolving computer capabilities that have crystallized these many disparate but information-based parts into a recognized “infrastructure.” Many significantly interested parties, or stakeholders, have crucial infrastructure interests because of the infrastructure’s pervasiveness and rapid expansion.

Table 1 highlights some of these stakeholders.

Federal Government	Public Servants
Military	Academia
The Economic Marketplace	International Economic Groups
Industries	International Political Groups
Industry Alliances	Labor Organizations
Congress	Local Governments
State Governments	Public Interest Groups
Regional Governmental Alliances	

Table 1. Typical Information Infrastructure Stakeholders⁷

These stakeholders cover a wide spectrum of the world environment. However, clearly this spectrum carries significant responsibility for the smooth running of the world environment, as a whole. Table 2 highlights some of the interests the stakeholders may have to ensure that their piece of the pie operates effectively. Stakeholders may share or uniquely hold these interests.

Universal Service	Regulation
Information Assurance	Privacy (Security)
Intellectual Property Rights	Spectrum Management
Interconnection	Standards and Protocols
Interoperability	Technologies
Ownership	User Education about Vulnerabilities
Pricing	User Friendly Interfaces
Jobs	National Security

Table 2. Typical Information Infrastructure Stakeholder Interests⁸

Tables 1 and 2 represent the guiding force for continued evolution of the information infrastructure. The evolutionary drivers from Table 1 represent the elements of national power: diplomatic, economic, military, social. As might be expected, this is not a homogeneous environment where all these stakeholders are in complete agreement relative to the issues of the information infrastructure. While the interests highlighted in Table 2 may pertain to one or more stakeholders, they may also include points of contention. For example, regulation, noted in Table 2, is important to Federal, State, Regional, Local Governments, Congress and Industry, but it is safe to say that their perspectives would be quite different. They would be responding to different motives, objectives and constituencies in addressing their particular aspect. It is this characteristic of the information infrastructure, a pervasive entity that influences many levels of society, that provides the basis for a more focused look at it relative to the industrial base.

The Industrial Base and the Information Infrastructure

The Clinton Administration's recent National Information Infrastructure Agenda for Action stated that:

Information is one of the nation's most critical economic resources....By one estimate, two-thirds of U.S. workers are in information-related jobs, and the rest are in industries that rely heavily on information. In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic importance to the United States.⁹

The combination of Tables 1 and 2 and the above quote clearly puts the U.S. industrial base, as a major stakeholder, in the middle of the GII. The GII encompasses the passageway for business and a significant business market. This situation is being driven by several factors, principal among them being the increasing globalization of the world economy and the exploding use of information technologies in conducting business operations.

The breakup of the Soviet Union, the continued emergence of China as a world trading partner, and the expansion of other Pacific Rim economies are but a few reasons that the global economy is growing rapidly. The meteoric advancement of information technology provides much easier access to the global marketplace for these emerging economies as well as the more established economies.. This worldwide marketplace brings increased competitiveness to obtain better market shares. Successful competition for an industrial player requires flexibility, adaptability, responsiveness, and advanced technological capabilities. For U.S. industry this global marketplace also dictates, at a minimum, competition against foreign businesses. Much more likely is foreign

partnering to provide the most competitive product. To compete in this environment means embracing and leveraging the information technology revolution.

Information technology is the key to leveraging the emerging global economy. To that end, U.S. businesses, during the 1980's, invested one trillion dollars in information technology. Information technology's positive impact on the trade balance currently is second only to the defense industry. Information technology will top the list by the end of the decade.¹⁰ Companies are increasingly relying on information technology to provide an efficient competitive advantage. One example of an internal contribution is Boeing's 777 airliner which has been widely touted as the first jetliner to be fully designed using three dimensional computer modeling technology that allowed the aircraft to be "pre-assembled" on the computer; thereby eliminating the need for a costly full scale mockup.¹¹ Companies recognize the value of information technologies not only for their internal contributions but for their external ones as well. External contributions, such as financial services, like banking, securities and commodities trading, letters of credit, currency conversions, and loan guarantees, make up approximately five percent of U.S. services exports. In mid-1992, the U.S. piece of the world financial services market was 66.3% with second place going to the United Kingdom at 17% followed by Japan with 5.1%.¹² Increasingly industry will be using information technology to link to consumers, partners, government agencies at all levels, foreign corporations and governments as the world economy becomes a more "local" environment. With the U.S. economy still a major force but not dominant, the U.S. will focus on being an engaged member of this global economy.

The information infrastructure and the industrial base are interdependent. It is difficult, if not impossible, to now imagine them being separate. They are pervasive, reaching all parts of the global society. Their expansion and information technology's advancement make the GII critical to the day to day operations of the national and global community and its economic prosperity. Just examining Tables 1 and 2 and contemplating the sense of those elements in an advancing technology environment provides an idea of how far reaching the infrastructure has become. This realization has, in recent years, driven the emergence and validation of an operational area at first known as Information Warfare and more recently known as Information Operations, as per the titles of Joint Pub 3-13 and FM 100-6 discussed earlier.

Information Operations

Joint Pub 3-13 defines Information Operations as those “actions taken to effect adversary information and information systems while defending one’s own information and information system.”¹³ Information operations, either offensive or defensive, encompass all levels of activity from peace to war. The focus of IO is “on the vulnerabilities and opportunities presented by the increasing dependence of the U.S. and its adversaries on information and information systems.”¹⁴ Examining Tables 1 and 2 again, it becomes clear that the stakeholders and their interests are at once the target of offensive IO and at the same time the subject for defensive IO. Industry and the Federal Government have interest in virtually all aspects of Tables 1 and 2 to some degree.

Protection and exploitation are the keywords that continue to focus our discussion in this article.

Our picture, thus far, is one of a vibrant, expanding, information infrastructure that increasingly touches all aspects of the global community. A key driver of this infrastructure is the global industrial community which has the information technology industry as a direct beneficiary and all industrial activities as customers as they search for the competitive edge and efficiencies in an ever smaller global marketplace. Information is quickly becoming the coin of the realm to the industrial community and thus making the GII both a revenue source and a pathway. The defense industry is an active member in this regard as it becomes more immersed in information technologies and dependent on the information infrastructure to compete in the increasingly competitive environment. Therefore, industry sees the GII as a necessary element for continued economic growth. A system that will house or carry significant sensitive data in ever widening circles and as an expanding marketplace itself. Encircling this entire picture is the IO concept of the government that encompasses both exploitation and protection of the information infrastructure in order to protect national security. The government and industry want much of the same information protected. However, the government also wants access for national security reasons and does not want foreign sources protected without access. From industry's perspective, the government wants to limit their market share and have undue access to sensitive data. The government, however, believes it needs to maintain the technological edge for national security purposes.

Cryptography's Not Just For Uncle Sam Anymore

Cryptography has long been the domain of the U.S. government in the protection of military and diplomatic information. The U.S. government cryptographic policy is one of protection and exploitation. First, is the protection of the U.S. military and diplomatic communications through cryptographic measures. Second, is the protection of its ability to access adversary information by controlling the export of cryptographic technology and technical data.¹⁵ The most significant environmental change affecting cryptography is the one embodied by the previous discussion of the changing face of national security and the industrial base. For U.S. industry, cryptography is rapidly becoming a necessity as a means of worldwide information protection and because industry worldwide has the same issue it also becomes a significant commercial product itself. Collectively, these perspectives provide elements of this cryptography situation that may not be wholly compatible.

Cryptography is at the heart of our discussion in the following pages.. Outlined below are several key points, from a recent National Research Council (NRC) study on cryptography.

Cryptography provides confidentiality through... an encryption algorithm and key... used to transform the original plaintext into the encrypted ciphertext. The strength of an encryption algorithm is a function of the number of steps, storage and time required to break the cipher and read any encrypted message, without prior knowledge of the key. Mathematical advances, advances in cryptanalysis, and advances in computing, all can reduce the security afforded by a cryptosystem... The strength of a modern encryption scheme is determined by the algorithm itself and the length of the key. For a given algorithm, strength increases with key size. However, key size alone is not a valid means of comparing the strength of two different encryption systems. Differences in properties of the algorithms may mean that a system using a shorter key is stronger overall than one using a longer key.¹⁶

Cryptography, when discussed from a confidentiality perspective, as is the case here, has “the characteristic that information is protected from being viewed in transit during communications and/or when stored in an information system.”¹⁷ As such, cryptography becomes an instrument for the protection of legitimate (government and industry) and illegitimate (adversarial governments or criminal activities) interests. Since both areas are expanding, the product potential for the cryptography market is significant. The increased market for cryptography products is contentious when considered against the government’s national security and law enforcement requirements.

The Industry Perspective

The industry perspective on cryptography is based on two basic points. First, that protection of the highly sensitive data, either traversing or stored with access to the GII, requires cryptographic capabilities. Second, that as a world leader in the information technology sector, the U.S. must achieve comparable status in cryptography or find its status eroding.

Protection of industrial data is becoming increasingly important to the members of the global marketplace. A mature GII, when coupled to a competitive world marketplace, increases the need to protect information and the difficulty in doing so. Potential adversaries may use this information to influence not only commercial but national security objectives. The National Counterintelligence Center (NACIC) concluded that “specialized technical operations (including computer intrusions, telecommunications targeting and intercept, and private sector encryption weaknesses)

account for the largest portion of economic and industrial information lost by U.S. corporations.¹⁸ Additionally, the NACIC reported that corporate communications, especially those with overseas locations, is highly susceptible to anyone wanting to obtain competitive information or trade secrets. This is increasingly true as many U.S. companies have started using electronic data interchange for electronically transferring corporate bidding, invoice and passing data overseas.¹⁹ Industry considers cryptography a vital requirement for protecting the confidentiality of information in worldwide business.

The U.S. is currently the leader in the world's information technology business area. This sector of the U.S. economy is the world's strongest with 8 of the world's top 10 application software vendors, the top 5 systems integration companies, 8 of the top 10 custom programming firms and the headquarters for the top 9 global outsourcing companies.²⁰ To maintain the U.S.'s lead and crucial role in the world technology sector, the U.S. must participate in all elements of the sector, this includes cryptography. U.S. leadership in the information technology field is based on quality, innovativeness, marketing and distribution expertise, research and product growth. These attributes require rigorous efforts to maintain this leadership. Leadership in this field is subject to public policy and industry action. As such, disharmony here can erode that leadership.²¹ The software business community, as represented by the Business Software Alliance (BSA), recently sent a letter to the Vice President of the U.S. expressing their concern over the Administration's cryptographic policy:

The American software industry needs immediate relief. It is a matter of jobs and international competitiveness. For the Administration's policy to be successful, the government must accept and work with the market, not try to supplant it. It is

clear that many in Congress understand the urgency and importance of this issue and the need for strong protection for Internet users.²²

BSA sent the letter in apparent frustration over the direction of U.S. cryptography policy.

U.S. export controls on cryptographic products and technical information severely limit availability of commercial cryptographic software on the world market. The Department of Commerce and the National Security Agency in a recent joint study found very few sophisticated cryptographic products from foreign companies and none from U.S. companies.²³ One industry estimate projects a potential \$30-60 billion loss of potential revenue to the U.S. information industry because of government restrictions on export of cryptography products.²⁴ Foreign competitors could easily fill the emerging void in this area..

The Government Perspective

The U.S. government cryptographic perspective has, since its inception, revolved around two basic concepts. First, that cryptographic measures protect U.S. military and diplomatic communications. Second, that controlling the export of cryptographic technology and technical data protects the government's ability to access adversary information.²⁵ Both of these concepts, while of critical importance, are feeling the pressure of the information technology explosion. The U.S. government is itself confronted with the changing face of national security as we discussed earlier. The GII and the Table 1 stakeholders and their emerging role as keystones to the national security picture complicate the issue. Protection of that information is, in many aspects, in the national security interests of the U.S. Therefore, strong cryptographic capabilities are

necessary to protect U.S. information worldwide. Strong cryptographic capabilities are available for domestic systems, but the impact of export controls adversely affects the availability of these capabilities in domestic products. This is a characteristic of a “globalized” economy. U.S. manufacturers, who cannot sell the full range of cryptographic products overseas, provide a lessor capability in U.S. products for production efficiency. This then provides a decreased degree of protection across that spectrum identified by the stakeholders.

The second issue for the U.S. government is one of access to the information infrastructure for national security or law enforcement purposes. This may be to exploit foreign government information or in certain cases to access domestic information where national security considerations are a factor. Protection of this capability has been through limited export of technology and technical data and consistent advancement efforts. These measures served two primary purposes: to delay the worldwide spread of strong cryptographic capabilities and their use and to provide a tool to monitor cryptography development since export intentions required review of products.²⁶ Though successful, the ability to continue to pursue this policy in the face of the information technology revolution and increasing economic power is certainly in question.

The Cryptography Policy Dilemma

The policy dilemma for the U.S. government is simply one of access. Protection of critical U.S. information on the GII is an absolute must for government and industry. However, the government’s long standing exploitation objective is now focusing on the

same information that U.S. industry considers as a lucrative market to protect. The critical type of U.S. information that requires protection on the GII is most likely the same for other countries as well. The government wants continued access to protected information. Industry's perspective is that the policy to ensure this edge in exploitation is jeopardizing their preeminence in the information technology field and costing them billions of dollars. While the root cause for the dilemma is simply access, the issues surrounding access are anything but simple.

Focus on Access

Access from a cryptography perspective has two elements: access through technically overpowering the cryptosystem and designed access. Both elements have roles in this policy dilemma. In both cases these elements are significant parts of the respective sides of this issue.

Technically overpowering the crypto system is breaking the cipher and reading any encrypted message without prior knowledge of the key. As we discussed earlier, this access is a function of the application of mathematics, cryptanalysis and computing power. Liberalization of export controls would diminish government's ability to rapidly access protected information for national security purposes. The reasons are two-fold: stronger encryption products on the market and the release of more advanced technical data. Other adversarial countries may use this technical data to enhance their cryptographic protection. Even breaking the code for a moderately strong key would take years with advanced general purpose computers.²⁷ The National Security Agency (NSA)

has recently joined with the National Institute of Standards and Technology (NIST), as a result of the Computer Security Act of 1987, to continue to review products and developments in the cryptography field.²⁸ Ambassador David Aaron, US Envoy for Cryptography in remarks on 28 January 1997, stated that there were national security risks to exporting stronger encryption capabilities. The Clinton Administration understood these risks and was willing to accept them to support a solution with key recovery.²⁹

Designed access is that capability placed into a cryptosystem to allow access to unprotected data. These may include maintenance and monitoring ports, master keys, key escrow or backup mechanisms or weak encryption defaults.³⁰ While all these design features allow the opportunity for unauthorized access, the key escrow and backup mechanisms provide the closest solution to the cryptography policy dilemma.

Key escrow or escrowed encryption, as it is also known, “refers to an approach to encryption that enables exceptional access to plaintext without requiring a third party (e.g., government acting with legal authorization,...an individual who has lost an encryption key) to perform a cryptanalytic attack.”³¹ Key escrow systems are developed with very strong cryptographic confidentiality against unauthorized third parties but none against those third parties that meet the requirements for exceptional access. This approach, from some perspectives, makes these systems inherently weak in cryptographic protection capabilities.³²

Key recovery is another type of key backup approach discussed concerning this problem. Key recovery is at the forefront of the cryptography policy dilemma because the government sees the potential for key recovery to solve the access dilemma. By one

definition, “key recovery is an approach that permits the recovery of lost keys without the need to store or ‘escrow’ them with a third party.”³³ This definition came from a 2 October 1996 joint press announcement by eleven major information technology vendors and user organizations, such as Apple, UPS, Digital Equipment Corporation, Sun Microsystems, and IBM. These groups formed an alliance to develop modern high-level key recovery solutions.³⁴ However, the different groups do not share a common understanding of key recovery’s definition. At the 5 December 1996 inaugural meeting of the Technical Advisory Committee (TAC) to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, the discussion of key recovery included trusted third parties, escrow/recovery centers and key recovery agents.³⁵ The TAC’s charter is to develop “an acceptable approach to key recovery while minimizing risk.”³⁶

Working on the Issues

Recent government and industry activities relative to cryptography seemed to hold promise for progress. A 1 October 1996 statement from the Vice President described an initiative that “will make it easier for Americans to use stronger encryption products--whether at home or abroad--...It will support the growth of electronic commerce, increase the security of the global information, and sustain the economic competitiveness of US encryption product manufacturers...”³⁷ The software industry, through the Business Software Alliance, cut the euphoria short by issuing a strong letter, previously quoted above, critical of the Administration’s actions in conjunction with the

announcement. BSA stated that "...significant backtracking has occurred..."³⁸ and that the government was now heading in the "...absolute wrong direction..."³⁹ A recent and striking example that, although both parties participated in extensive discussions prior to the announcement, significant miscommunication was still possible. It appeared that different perspectives and objectives caused confusion even though a technology solution may be possible to protect both interests. Thus the policy dilemma posed by cryptography continues.

Foreign governments also play a part in the policy dilemma. As sovereign governments and stakeholders in the GII, Tables 1 and 2 discussed earlier, are most certainly mirror images from their perspective. A big difference in perspective is that these countries are not at the top in the information technology sector as is the U.S. Ambassador Aaron, after face to face meetings with many countries, synopsized their views. He found that:

- all appreciated the importance of encryption
- all recognized the need for international cooperation
- all supported lawful access by governments
- many countries wanted stronger controls than the U.S. has
- almost all disapproved of U.S. exporting stronger encryption products and some criticized U.S. lack of internal controls
- all were concerned that stronger products created domestic protection problems for them
- many believed that commercial advantage was driving the U.S. policy

-all were willing to develop a global key management structure⁴⁰

Clearly, there is a mixed bag in terms of international reaction. The main international points are: they also see an absolute need for action, that like it or not they see the U.S. leading the effort, and they support the absolute need for legitimate government access.

The Computer Systems Policy Project (CSPP) is an information technology industry group that develops and advocates public policy positions on trade and technology issues. The CSPP includes the Chief Executive Officers (CEOs) from companies such as: Compaq, Data General, Digital Equipment, Hewlett Packard, and IBM. A recent CSPP study, "Perspectives on Security In the Information Age," offered several policy recommendations as first steps towards a comprehensive policy:

1. Link the decontrol of U.S. commercial cryptographic products to the availability of competitive products in the international marketplace.
2. Permit export of stronger U.S. commercial cryptographic products, without technology restrictions for legitimate commercial end users, unless the government clearly demonstrates a risk.
3. Discuss the export of stronger U.S. commercial cryptographic products that meet reasonable government access needs.
4. Embargo U.S. commercial cryptographic products in terrorist countries.⁴¹

The National Research Council is an arm of the National Academy of Sciences, "a private, nonprofit, self-perpetuating society... engaged in scientific and engineering research...the Academy has a mandate that requires it to advise the federal government on scientific and technical matters."⁴² The NRC formed the Committee to Study National Cryptographic Policy in November 1993 at the request of Congress. The Committee published a comprehensive and extensive study, "Cryptography's Role in Securing the Information Society," in 1996. The study outlined the following recommendations:

1. No law should bar the manufacture, sale or use of any form of encryption within the U.S.
2. National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of the law.
3. National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces.
4. Export controls on cryptography should be progressively relaxed but not eliminated.
5. The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age.
6. The U.S. government should develop a mechanism to promote information security in the private sector.⁴³

The two studies' recommendations have some similar elements but in some predictable areas they are different. Both studies recommend that the government policy reflect the direction of commercial cryptography market forces. Both studies discuss export controls but have slightly different perspectives. NRC recommends a gradual relaxation of export controls but not elimination. CSPP, an industry group, takes a predictably less stringent approach by calling for the export of stronger cryptographic products without technology restrictions unless the government proved a risk.

What Should the U.S. Do?

What should the U.S. do? A difficult question to answer because, as we have seen, the dilemma presented by cryptography is complex. What is clear is that when the question refers to "the U.S." it does not focus solely on government or industry. The interests of both parties are so interdependent so that choosing one over the other is not viable. However, as the discussion involves a policy question, ultimately the U.S. government must utter words or present statements that establish this policy. Industry's key role in the success of any policy and the impact of such a policy on the overall health

of U.S. dominance in the information technology sector is not lost on the government. It makes the policy more important and more difficult to develop.

The government and industry are both dependent on the pervasiveness of the GII and the exploding growth of the information technology sector. These are key elements of national power for the U.S. government. They interconnect the emerging global economy and position the U.S. as a dominant force in the field. They are also key elements for industry in order to excel in the global economy and continue to be a dominant force in this technology sector. While at this level it might appear that industry and the government have similar objectives, the injection of cryptography into the discussion brings to the forefront the differences between these two players. The key difference revolves around access. The government demands access to protected information and protection from unwanted access for both government and industry sensitive data. Industry is cautious about the government's desire for access. Industry demands unrestricted access to the competitive market place and protection for its sensitive data. Government, for its part, is cautious of industry's requirement for unrestricted access. These different perspectives plus the perspectives of other stakeholders, most notably foreign governments and businesses, create an environment where a cryptography policy will most likely not have total consensus agreement. While total agreement is not a necessity, cooperation and compromise are necessary to protect both interests.

The U.S. must develop a cryptographic policy that incorporates the different perspectives involved and reflects the issues discussed above. However, at a minimum

the policy requires two elements: government access and U.S. industry pre-eminence in the information technology field. Neither should eclipse the other. As these are not wholly compatible objectives some form of compromise will be necessary in achieving a coordinated joint policy.

Government access to protected data is absolutely critical for national security purposes. The information age encompasses a broader spectrum of national security interests such as critical national infrastructure systems (communications, power, transportation, financial). This coupled with expanded cryptography usage in many non-government related fields necessitates a mechanism for legitimate government access. Some type of key recovery is the optimum choice. This assumes, of course, that the government and industry can agree on the definition and structure of the key recovery system. Industry's position is that key recovery with third party access inherently weakens the strength, and thereby the marketability, of any cryptographic product. Ambassador Aaron's assessment, based on discussions with many governments, concluded that key recovery will eventually be an international requirement.⁴⁴ An international requirement for key recovery will ease the government's difficulty on the policy side by leveling the competitive playing field from the industry perspective. U.S. industry will not have to be concerned that foreign competitors will be selling stronger cryptography with no key recovery because there will be no market.

Pre-eminence of U.S. industry in this increasingly vital part of the information technology sector is the second key element. The positive national security aspects of being the dominant force in the global information technology sector and the significant

economic benefits are powerful reasons for continued U.S. dominance in this field. Continued support for a global key recovery regime is critical in order to level the playing field for the U.S. industry. Export controls are a key element in the protection of the government's access ability. As such, the government should focus on coordinating with industry the relaxation not elimination of export controls. This coordination should take into account the current availability of cryptography products to ensure U.S. competitiveness. The level of technology exported requires a careful balanced approach. Government's too conservative approach will, in the long run, be as detrimental to the economic side of U.S. national security interests as will a too liberal export policy.

The government must lead this effort. It is a government policy formulation effort, therefore the lead cannot rest elsewhere. It is not prudent to take one side or the other in this matter because both the government and industry perspectives have merit. The pathway to solving this problem requires a team approach with each partner reaching their respective objectives. The separate industry groups, such as BSA or CSPP, add little because their perspective is wholly industry with little government perspective. The government must continue to press through Ambassador Aaron, as well as other forums, for the incorporation of a global key recovery requirement. For their part, industry must continue to dominate the information technology sector and continue to enhance the sophistication of the cryptographic systems, to include key recovery. The ability of the government to attain a global agreement on key recovery and the continued dominance of U.S. industry in the information technology sector to include cryptography will go a long way to fulfilling a successful policy from all perspectives. A continued dialog with industry over export controls is critical, as this will be a sensitive area. However, the

government must be able to technically overwhelm protected systems if necessary for national security purposes. A permanent government-industry team is necessary to continue to focus issues and ensure that all perspectives are considered.

Conclusion

Cryptography is an “old” emerging technology. An old technology that is emerging from a predominantly intelligence and national security environment to a more general worldwide environment. The solutions to the policy issues resulting from this emergence will not satisfy everyone. Good and valid reasons support the many perspectives. As is often the case, the “solution” is not really a solution but more a continual balancing act to minimize the damage to all the parties involved. Cryptography falls in this area. The U.S. must maintain its lead in the information technology sector for national security and economic reasons. The ability for the government to legitimately access protected data is also critical. A progressive cryptography policy of government and industry coordination is essential to meeting both objectives. It will be critical in the future information based environment.

ENDNOTES

¹ Joint Chiefs of Staff, Joint Doctrine for Information Operations (First Draft) (Washington, DC: Joint Chiefs of Staff, 1997), I-23.

² Ibid, I-24.

³ Ibid, I-25.

⁴ Colonel Michael D. Starry and Lieutenant Colonel W. Arneson, Jr, "FM 100-6: Information Operations," Military Review 6 (November-December 1996): 5.

⁵ Ibid.

⁶ Ibid.

⁷ Joint Chiefs of Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2d Edition (Washington, DC: National Defense University, 4 July 1996), 2-17.

⁸ Ibid.

⁹ "Information in the Global Economy," undated, <<http://www.annenberg.nwu.edu/pubs/global/global11.htm>>, 28 February 1997.

¹⁰ Ibid.

¹¹ Boeing Aircraft Company, "777 Computing Design Facts," February 1997, <http://www.boeing.com/bck_html/boe777comp.html>, 22 February 1997.

¹² Information in the Global Economy.

¹³ Joint Pub 3-13, I-1.

¹⁴ Ibid, I-2.

¹⁵ Kenneth W. Dam and Herbert S. Lin, Editors, Cryptography's Role in Securing the Information Society (Washington, DC: National Academy Press, 1996), 4.

¹⁶ U.S. Congress, Office of Technology Assessment, Information Security and Privacy in Network Environments, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994), 112.

¹⁷ Cryptography's Role, 54.

¹⁸ Ibid, 31.

¹⁹ Ibid, 31.

²⁰ Ibid, 38.

²¹ Ibid, 38-40.

²² Business Software Alliance, "BSA Letter to the Vice President," 2 December 1996.

²³ Cryptography's Role, 128.

²⁴ Computer Systems Policy Project, "Perspectives on Security in the Information Age," January 1996. <<http://www.cspp.org/reports/report1-96.html>>, 15 January 1997.

²⁵ Cryptography's Role, 4.

²⁶ Ibid, 114.

²⁷ Electronic Privacy Information Center, "US Cryptography Policy: Why We Are Taking the Current Approach," 12 July 1996, <<http://www.tis.com/docs/products/recoverkey>>, 15 March 1997.

²⁸ Cryptography's Role, 236.

²⁹ Ambassador David Aaron, "International Views of Key Recovery," Statement presented at RSA Data Security Conference, 28 January 1997, <<http://www.bxa.doc.gov/aaron.htm>>, 15 March 1997.

³⁰ Cryptography's Role, 57.

³¹ Ibid, 169.

³² Ibid.

³³ Electronic Privacy Information Center, "Joint Press Announcement: High-Tech Leaders Join Forces to Enable International Strong Encryption," 2 October 1996, <<http://www.tis.com/docs/products/recoverkey>>, 22 February 1997.

³⁴ Ibid.

³⁵ Department of Commerce, "Minutes of the 5-6 December 1996 Meeting of the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure," <<http://csrc.nist.gov/tacdfipsfkmi/minutes9612.txt>>, 15 March 1997.

³⁶ Ibid.

³⁷ The White House, Office of the Vice President, "Vice President on Clipper 4," 1 October 1996.

³⁸ BSA Letter.

³⁹ Ibid.

⁴⁰ Ambassador Aaron.

⁴¹ CSPP.

⁴² Cryptography's Role, vi.

⁴³ Ibid, 303-335.

⁴⁴ Ambassador Aaron.

BIBLIOGRAPHY

Aaron, Ambassador David. "International Views of Key Recovery." Statement presented at RSA Data Security Conference. 28 January 1997,
<<http://www.bxa.doc.gov/aaron.htm>>. 15 March 1997.

Boeing Aircraft Company. "777 Computing Design Facts." February 1997,
<http://www.boeing.com/bck_html/boe777comp.html>. 22 February 1997.

Business Software Alliance. "BSA Letter to the Vice President." 2 December 1996.

Computer Systems Policy Project. "Perspectives on Security in the Information Age." January 1996. <<http://www.cspp.org/reports/report1-96.html>>. 15 January 1997.

Dam, Kenneth W. and Herbert S. Lin, Editors. Cryptography's Role in Securing the Information Society. Washington, DC: National Academy Press, 1996.

Department of Commerce. "Minutes of the 5-6 December 1996 Meeting of the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure."
<<http://csrc.nist.gov/tacdfipsfkmi/minutes9612.txt>>. 15 March 1997.

Electronic Privacy Information Center. "US Cryptography Policy: Why We Are Taking the Current Approach." 12 July 1996,
<<http://www.tis.com/docs/products/recoverkey>>. 15 March 1997.

Electronic Privacy Information Center. "Joint Press Announcement: High-Tech Leaders Join Forces to Enable International Strong Encryption." 2 October 1996,
<<http://www.tis.com/docs/products/recoverkey>>. 22 February 1997.

"Information in the Global Economy," undated,
<<http://www.annenberg.nwu.edu/pubs/global/global11.htm>>, 28 February 1997.

Joint Chiefs of Staff. Joint Pub 3-13, Joint Doctrine for Information Operations (First Draft). Washington, DC: Joint Chiefs of Staff, 21 January 1997.

National Defense University. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance 2d Edition. Washington, DC: National Defense University, 4 July 1996.

Starry, Colonel Michael and Lieutenant Colonel W. Arneson, Jr. "FM 100-6: Information Operations." Military Review 6 (November-December): 2-15.

The White House. Office of the Vice President. "Vice President on Clipper 4." 1 October 1996.

U.S. Army Field Manual. FM 100-6, Information Operations. Washington, DC: U.S. Government Printing Office, August, 1996.

U.S. Congress, Office of Technology Assessment. Information Security and Privacy in Network Environments, OTA-TCT-606. Washington, DC: U.S. Government Printing Office, September, 1994.